It's all about relationships

Use generative AI and knowledge graphs to comply with global data and privacy requirements at scale

With the passage of India's Digital Personal Data Protection Act ("DPDPA") and seven additional US state consumer privacy laws, 2023 represents another challenging year for meeting dynamic global data and privacy regulatory requirements. Is your organization built to sustainably manage the fast-changing requirements at scale?[1,2]

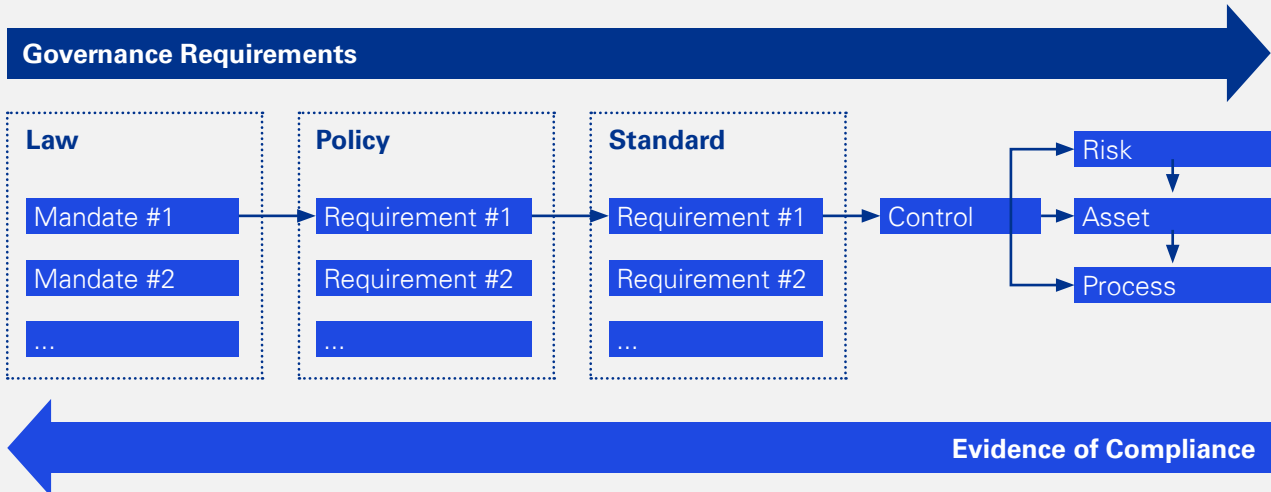### Developing a data model consistent with regulatory compliance

Ideally the connections between data and privacy regulatory requirements, policies and standards, and the risk and control environment would be well-modeled, so that the relationships between them are understood, tracked and managed. When organizations maintain these relationships, it is possible to understand how new data and privacy requirements are being addressed by corporate policy and in operations across the enterprise at any given time. Further, it simplifies analysis and reporting of the impact of new or revised requirements.

> "
>
> **Achieving data and privacy compliance and risk management at scale requires organizations to model and manage relationships across the data risk ecosystem. But this is often an afterthought for many organizations—to their detriment. "**
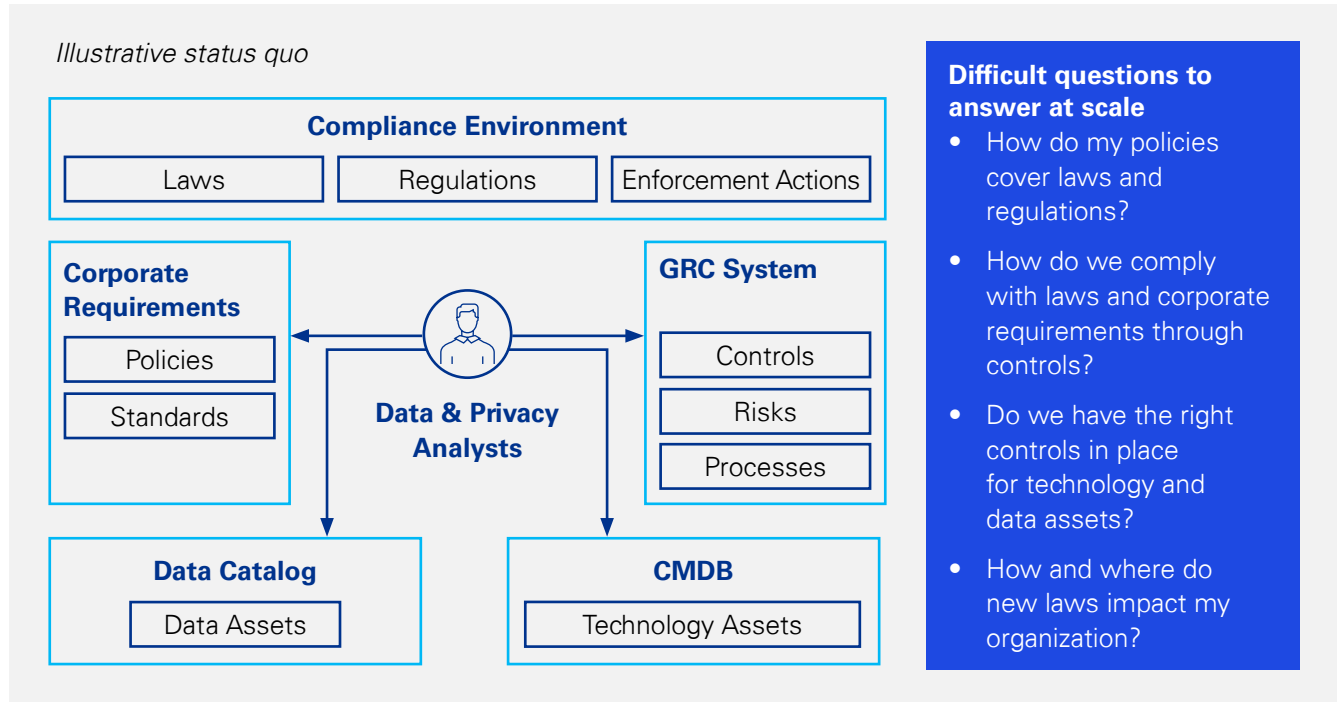>
> Steven Stein
> Principal, Privacy

Illustrative ideal model

Governance Requirements

Law	Policy	Standard		
Mandate #1	Requirement #1	Requirement #1	Control	Risk
Mandate #2	Requirement #2	Requirement #2		Asset
...	...	...		Process

Evidence of Compliance

The status quo for many organizations is not built for scale and sustainability

In many organizations, however, this model is never established or becomes unwieldy to maintain due to the lack of technology enablement. The problem is exacerbated by the sheer volume of laws, regulations and enforcement actions; numerous policies owned by different executives (e.g., CPO, CISO, CDO, CRO, GC); poor or incomplete data in Governance, Risk, and Compliance (GRC) systems, data inventories and configuration management databases ("CMDBs"); and lack of defined relationships between them. The data and privacy regulatory compliance model is disorganized and managed in a manual, ad hoc fashion by data risk analysts. It tends to look closer to the diagram below.

Illustrative status quo

Compliance Environment

| Laws | Regulations | Enforcement Actions |

Corporate Requirements
- Policies
- Standards

Data & Privacy Analysts

GRC System
- Controls
- Risks
- Processes

Data Catalog
- Data Assets

CMDB
- Technology Assets

Difficult questions to answer at scale
- How do my policies cover laws and regulations?
- How do we comply with laws and corporate requirements through controls?
- Do we have the right controls in place for technology and data assets?
- How and where do new laws impact my organization?

The status quo is typically managed by people without the support of technology, which often results in unacknowledged policy and control gaps. The organization never fully understands its compliance and data risk management posture across the entire data and technology estate. Value is wasted as analysts conduct ad hoc, manual analyses to answer point-in-time questions (e.g., legal change impact, audit/exam preparation, event response) that quickly go stale.

Use generative AI and graph technology to manage data and privacy relationships

Generative artificial intelligence ("GenAI") and graph databases are two technologies that enable managing data risk relationships and addressing regulatory change at scale. The below conceptual architecture shows these technologies as a single solution to automate converting laws and policies into discrete requirements and connecting their relationships to the broader data privacy risk management ecosystem (e.g., controls, processes, assets).
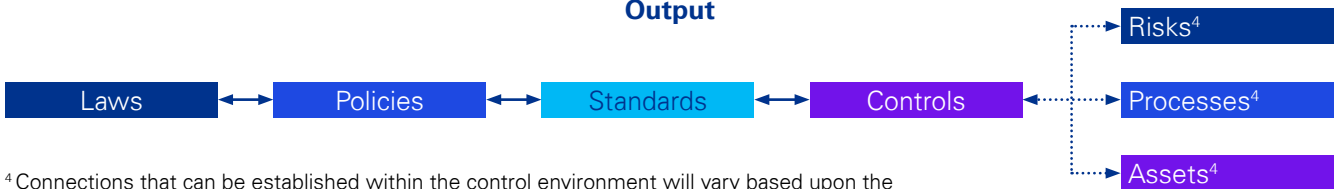
It's all about relationships

1. Upload structured and unstructured data

2. Send series of queries and data passed to Generative AI through API calls

3. Return automatically parsed unstructured data into structured data and matched result

4. API call to request additional data already stored in graph database

5. Returns responsive data

6. User validate matches[3] and writes entities and relationships to graph database
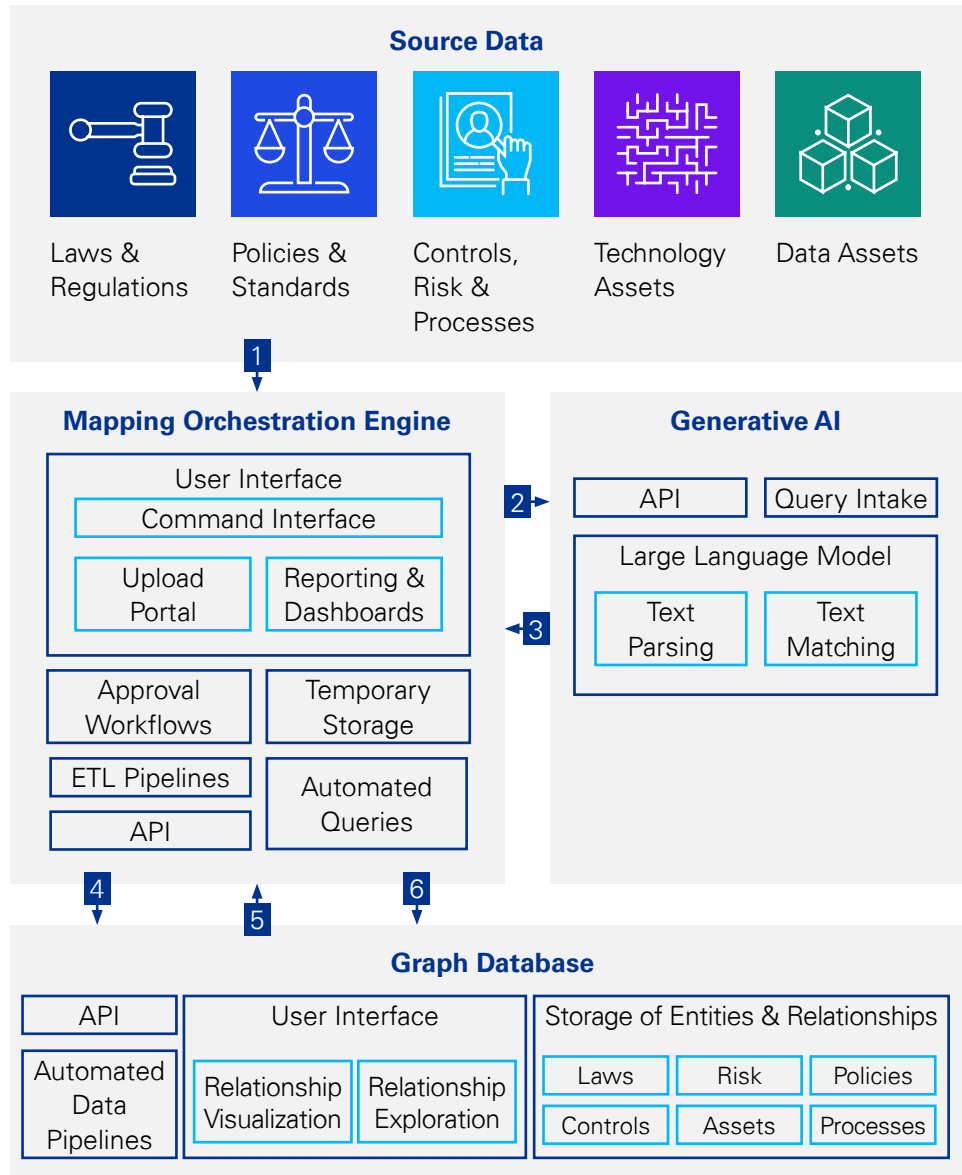
[3] A series of additional API calls to Generative AI may be conducted for additional relationship mapping

Source Data

Laws & Regulations

Policies & Standards

Controls, Risk & Processes

Technology Assets

Data Assets

1

Mapping Orchestration Engine

User Interface

Command Interface

Upload Portal

Reporting & Dashboards

Approval Workflows

Temporary Storage

ETL Pipelines

API

Automated Queries

Generative AI

API

Query Intake

Large Language Model

Text Parsing

Text Matching

2

3

4

5

6

Graph Database

API

Automated Data Pipelines

User Interface

Relationship Visualization

Relationship Exploration

Storage of Entities & Relationships

Laws

Risk

Policies

Controls

Assets

Processes

Output

Laws ↔ Policies ↔ Standards ↔ Controls

Risks[4]

Processes[4]

Assets[4]

[4] Connections that can be established within the control environment will vary based upon the organization's existing known relationships or ones that can be inferred.

Two usage paths and nearly limitless use cases

The combined solution can help to organize the existing data relationships and manage the relationships going forward to enable sustainable and scalable data and privacy compliance and risk management.

It's all about relationships

1. Drives Organization of Data & Privacy Relationships

Automated Text (Laws/Policies) Parsing

GenAI-Assisted Mapping/Matching

Structured and Orderly Human Review Process

Requirement Inventory Linked to Control Environment

Approval Audit Trails

2. Enables Ongoing Data & Privacy Relationship Management.

Control Coverage Analysis

Policy Coverage Analysis

Regulations Coverage Analysis

Scenario Change Analysis

Risk Aggregation & Quantification

How KPMG can help

We have the proven experience and U.S. patent pending solution to help you design, implement and operate these technologies to address your data and privacy regulatory compliance and control coverage needs:

- **Mapping Orchestration Engine:** low-code solution for streamlining the uploading of data and querying GenAI API

- **Optimized GenAI Queries:** pre-built and optimized GenAI queries to obtain accurate text parsing and mapping results

- **Intelligent Graph UI:** visualization layer that enables intuitive exploration of the graph database entities and relationships between them

- **Tested data model:** data model organizing the relationships across the data privacy risk ecosystem

- **Implementation experience:** successful design, implementation and deployment of these solutions at large Fortune 100 organizations

"

Organizations are faced with an onslaught of requirements on their data—regulatory (e.g., privacy, liquidity, capital) or otherwise. Addressing these requirements in a comprehensive, practical and efficient manner requires the ability to understand the interconnections across the governance, technology and data estate. "

Pedro Calado
Managing Director, FS Data

Our team of privacy professionals, technologists, and data scientists can help your organization react to the dynamic regulatory compliance environment by organizing your data and privacy relationships for scalability and sustainability.

Contact us

Steven Stein
Principal, Privacy, Advisory, KPMG LLP
T: +1 312 952 3110
E: ssstein@kpmg.com

Pedro Calado
Managing Director, FS Data, Advisory, KPMG LLP
T: +1 313 230 3062
E: pcalado@kpmg.com

Michael Henzey
Director, Privacy, Advisory, KPMG LLP
T: +1 571 635 4336
E: mhenzey@kpmg.com

Jim Leach
Director, Lighthouse, Advisory, KPMG LLP
T: +1 770 240 8707
E: jimleach@KPMG.com

Source 1 (endnote for the passage of the DPDPA): "The Digital Personal Data Protection Act of India, Explained," Raktima Roy and Gabriela Zanfir-Fortuna, Future of Privacy Forum (August 15, 2023).

Source 2 (endnote for the passage of the seven additional US state consumer privacy laws): "US State Privacy Legislation Tracker," International Association of Privacy Professionals (September 15, 2023).

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia